RSAConference™

CISO PERSPECTIVES

How Top CISOs Are Transforming Third-Party Risk Management

Exclusive Insights from the RSAC Executive Security Action Forum (ESAF)

A Message from the RSAC ESAF 2023 Program Committee

As a forum for candid discussion among peers, ESAF sessions are confidential, invitation-only, and limited to a select group of senior-most information security and risk executives. This year ESAF is celebrating its 20th anniversary. We mark this occasion by sharing some hard-earned wisdom with the broader cybersecurity community through a series of reports on topics of interest to all information security executives. Through these reports, we aim to help all organizations improve the management of cyber risks.

For more information on ESAF, see *www.rsaconference.com/ESAF*

The RSAC ESAF 2023 Program Committee includes:

Zaki Abbas, Senior Vice President, Chief Information Security Officer, Brookfield Asset Management
Brad Arkin, Senior Vice President, Chief Security and Trust Officer, Cisco
Jason Barnett, Vice President, Chief Security Officer, HCA Healthcare
Benjamin Brophy, Group Chief Information Technology and Security Officer, Reckitt Benckiser Group
Deneen DeFiore, Vice President & Chief Information Security Officer, United Airlines
Jerry Geisler, Senior Vice President and Chief Information Security Officer, Walmart
Richard Hale, Global Chief Information Security Officer, Sony Group Corporation
Gary Harbison, Chief Information Security Officer, Johnson & Johnson
Katie Jenkins, EVP for Global Cybersecurity and Chief Information Security Officer, Liberty Mutual Insurance
Michael Johnson, Chief Information Security Officer, Meta Financial Technologies, Meta
Catherine McCully, Chief Information Security Officer, Procter & Gamble
Michael McNeil, Senior Vice President, Global Chief Information Security Officer, McKesson
John Scimone, President and Chief Security Officer, Dell Technologies
Emma Smith, Chief Information Security Officer, Vodafone
Kevin Tierney, Vice President and Chief Cybersecurity Officer, General Motors
Howard Whyte, Executive Vice President and Chief Information Security Officer, Truist Financial Corporation
JR Williamson, Senior Vice President and Chief Information Security Officer, Leidos

RSAC™
Executive Security Action Forum
A Community of Fortune 1000 CISOs

About RSAC ESAF

The Executive Security Action Forum (ESAF), an RSA Conference (RSAC) community, has been a trusted forum for Fortune 1000 Chief Information Security Officers (CISOs) since 2003. Led by a program committee, the community shares information at confidential sessions throughout the year and at our annual meeting at RSA Conference, enabling security leaders at some of the world's largest enterprises to collaborate and find actionable solutions to common challenges.

Contents

Bold New Approaches Aim to Change Standard Practice

The consensus in the ESAF community of CISOs is that traditional third-party risk management in information security is ineffective. Traditional methods, centered around self-assessment questionnaires and cybersecurity ratings, do not provide an accurate picture of third-party risk nor reduce risk.

The need for change is growing more urgent as attackers increasingly target third parties. ***In a recent survey, RSA Conference found that 87% of Fortune 1000 companies were affected by a significant cyber incident at a third party in the past 12 months.***[1]

Third-party incidents can have a huge impact on the bottom line. If a supplier or business partner is hit with a cyber attack, it can disrupt the company's operations and/or expose the company's customer data or intellectual property. Attackers can also use third-party access as a route to infiltrate the company's network.

Although third-party risk management needs an overhaul, fixing it can seem like an intractable problem. Traditional approaches have become entrenched as standard practice, so companies are under pressure to continue using them even though they are ineffective.

Motivated by escalating risks, CISOs within the ESAF community are taking bold new approaches. These include establishing top priority security requirements, setting deadlines to implement controls, adding enforcements to contracts, helping third parties obtain security technologies and services, increasing the role of business leaders, and building resiliency against third-party incidents.

This report covers pioneering initiatives at six Fortune 1000 companies in a range of industries: defense, healthcare, insurance, manufacturing, and technology. It shares their journeys with the hope that others can use these ideas to accelerate their own efforts. Recognizing the need for systemic changes, this report also explores the roles of technology and security vendors, industry collaborations, and governments.

> *"The traditional way most organizations do third-party risk management is like security theater. There are thousands of people working ferociously, increasing the cost profile of businesses, but not actually decreasing risk. We have to challenge ourselves to stop wasting money, stop wasting time, stop pretending, and ask, 'Where could we make investments that could actually meaningfully buy down risk?'"*
>
> **John Scimone**
> **President and CSO**
> **Dell Technologies**

How to Use This Report

For CISOs, this report contains food for thought about what change is possible and how other CISOs have made it happen.

For executives and business leaders who work with CISOs to manage cyber risk, it sheds some light on the issues and possible ways to drive changes.

For companies of all sizes that are suppliers or partners to large enterprises, this report serves as an indicator of how expectations for third parties are changing.

For technology and security vendors, industry collaborations, and governments, it provides ideas on how they can make a difference.

[1] Based on a survey of 100 Fortune 1000 CISOs conducted by RSA Conference for an internal research study in Q2 2023.

A Rare Glimpse into Groundbreaking Efforts at Fortune 1000 Companies

Research Methodology

This research is based on discussions over a series of ESAF meetings and follow-up interviews with ESAF CISOs. The content reflects the perspectives of CISOs from across the ESAF community.

It features six in-depth case studies from a diverse set of Fortune 1000 companies, describing how these leading companies are transforming third-party risk management. At confidential ESAF sessions, these CISOs candidly shared their stories with their peers. They presented new approaches in third-party risk management, including some initiatives at very early stages, and garnered support and feedback.

To enable the sharing of highly sensitive information, we have fully anonymized all findings. Our commitment to anonymity allows this report to describe not only successes but also internal challenges and unresolved issues.

Members of the ESAF Program Committee guided the analysis and added their own insights. The quotes throughout the report are their reflections on the topic.

Definition of Third Party

The companies covered in this research each have thousands of third parties including:

- Suppliers of:
  - Software and hardware for IT or OT (operational technology) environments.
  - Devices and equipment.
  - Components used in the company's products.
- Service providers such as:
  - IT/cloud/SaaS.
  - Facilities maintenance.
  - HR, finance, and payroll.
  - Manufacturing.
- Distributors, dealers, brokers, and/or agents.
- Business partners.

"For years, this seemed intractable. Now we might be starting to move the needle. We're at a place where we are all doing more. Hearing what others are doing is always interesting — they might have cracked the nut."

JR Williamson
SVP and CISO
Leidos

Part I: The Need for New Approaches

Escalating Third-Party Risk

In all sectors, CISOs across the ESAF community are seeing that cyber attacks against third parties are increasing. There are several factors behind this trend including:

- If an attacker's ultimate goal is to obtain a Fortune 1000 company's data or access to its systems, an easier route can be to target the company's third parties. Large global enterprises have developed sophisticated cyber defenses, while their third parties often have less mature security programs.
- Even if an attacker's intended target is not specifically a Fortune 1000 company or its third parties, cyber attacks, especially ransomware attacks, are so rampant, a growing number of third parties are getting hit.
- Attackers are finding software or hardware providers can be attractive targets. By breaking into the provider's system and tampering with their product or service, an attacker can potentially compromise all the organizations which use the product or service.

When a third party is breached, a company may experience business disruption due to third-party downtime, lose data they had shared with the third party, suffer an attack on their corporate network, and/or face additional scrutiny from regulators and auditors.

Attacks on third parties are dramatically driving up risks for enterprises. ***One of the companies in our research saw third-party incidents rise 550% in three years.*** At many companies, third-party cybersecurity risk is now one of the top risks facing the enterprise and a major concern for executive leadership and the board of directors.

> *"Everyone's tolerance for risk is different. Even being conservative, I believe it's safe to say that third parties account for a significant portion of cyber events."*
>
> **Jason Barnett**
> **VP, CSO**
> **HCA Healthcare**

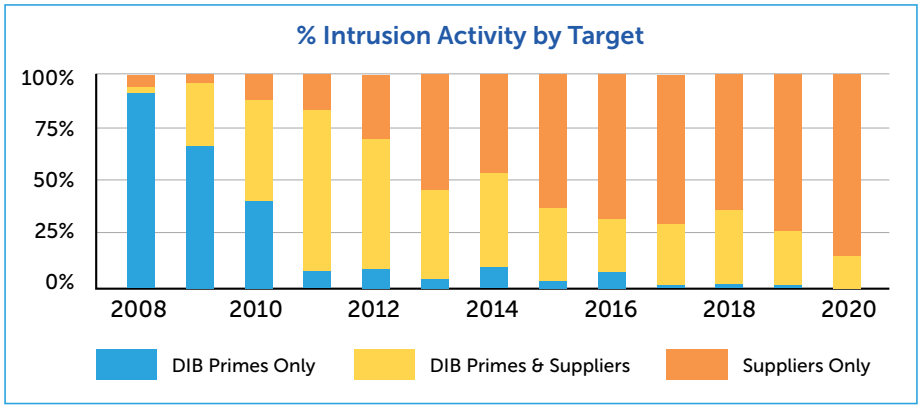


Figure 1: According to U.S. defense industry internal research, attackers have moved from targeting Defense Industrial Base prime contractors (DIB Primes) to suppliers. Similar trends have been seen in all sectors.

Limitations of Traditional Approaches

Traditionally in information security, most third-party risk management efforts are focused on assessing the third parties' security controls using self-assessment questionnaires, cybersecurity rating services, and sometimes compliance framework reports. The CISOs in the ESAF community see many limitations with these methods, as described in the table below:

Assessment Method	Limitations
Self-Assessment Questionnaire Lengthy list of questions asking the third party to declare they have security controls in place. • Often 200+ questions • Typically done on an annual basis	• Attesting to a checklist of controls is a poor indicator of good security. – A company can claim to have controls in place yet have very weak controls. • For example, for the question, "Do you do security awareness training?", a company that sends employees a security reminder email once a year might say yes. • Checklists are commonly completed by people lacking security knowledge (e.g., a supplier's salesperson). • If security gaps are identified, often they are not remediated; instead, they are documented and tracked. • A checklist approach to information security is considered too focused on compliance rather than managing risks.
Cybersecurity Ratings A commercial service provider rates an organization's security posture based on external scanning of the third party's network.	• The ratings are not a meaningful representation of an organization's security posture: – Ratings are based on a loose interpretation of publicly available data. – Scans provide no visibility into the third party's internal controls, mitigations, or capabilities. • The appeal of ratings is having a quantitative method to measure security posture, but CISOs do not have much faith in the numbers.
Compliance Framework Report A report provides an assessment of the third party's security program against a framework of controls such as SOC 2.[2]	• Often a self-assessment rather than a report by an external auditor. • The quality varies; very few are based on onsite audits and controlled testing. • The scope of the report is often not comprehensive (e.g., only one system may be in scope).

[2] Service Organization Control Type 2 (SOC 2) is a cybersecurity compliance framework developed by the American Institute of Certified Public Accountants (AICPA).

Traditional approaches have become expected as due diligence, especially in case of liability and/or as part of a cyber insurance assessment. However, these approaches:

- **Do not reduce risk.**
  - Are inherently focused on assessment rather than risk reduction.
- **Do not provide an accurate measure of security posture.**
  - Are based on imprecise data from self-assessments and external scans.
- **Waste huge amounts of time and money.**
  - Involve a labor-intensive process to collect, review and follow up on questionnaires from thousands of third parties.
  - Are hard to automate due to the lack of standardization.
- **Lack cyber risk context.**
  - Do not consider the specific type of cyber risks involved, such as customer data breach or supply chain disruption.
- **Lack resiliency strategies.**
  - Do not prepare companies for inevitable third-party security failures.
- **Generate a lot of work for third parties.**
  - Expect them to do ongoing lengthy assessments and audits which can be disruptive to their operations.
- **Create enormous duplication of effort for third parties.**
  - Require them to fill out a different questionnaire for each customer or business partner (each one has their own version).
- **Do not help third parties achieve effective security, as discussed in the next section.**

Third Parties Struggling with Security

The companies in our case studies have engaged with thousands of third parties through incident root cause analyses, focus groups, and surveys. The issues their third parties experience are summarized below.

Can't Afford Security

To protect today's digital environments, a minimum set of preventive and detective controls needs to be in place which requires cyber expertise across a wide range of skills plus the latest security technologies. CISOs estimate this requires at least $2 million to $5 million USD per year. Many organizations, especially small to mid-sized businesses (SMBs), can't afford it.

Can't Make It Work

Even if third parties are able to increase their security budget, they face other hurdles to effective security such as:

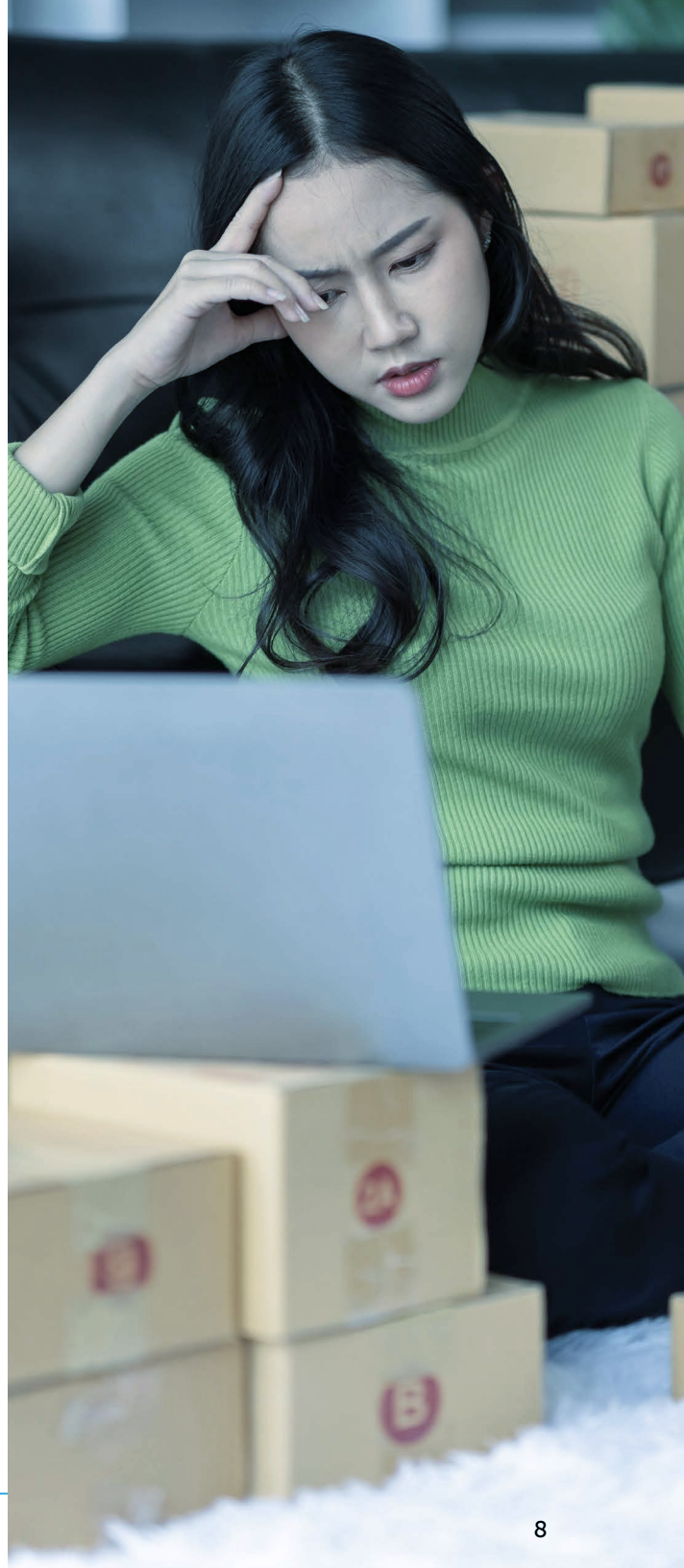
- They must comply with complex industry standards and government regulations which are often so complex it's difficult to determine a meaningful set of requirements.
- Commercial security solutions are often not appropriate for their use cases.
- The convoluted security marketplace makes it difficult to select and integrate controls.
- They have specialized and/or legacy systems or equipment that is difficult to secure.
- They can't find and retain cybersecurity talent.
- They perceive security as being difficult even when there are relatively simple things they could do, such as multi-factor authentication (MFA) for remote access.

Get Pulled in Other Directions

- Third parties can spend inordinate amounts of time on assessment questionnaires and audits, leaving little time for staff to do actual security.
- Some companies may calculate that the cost of losing a few customers or business partners is less than the cost of becoming secure.

> *"We are asking: How do we stop this paper chase of questionnaires and assessments? This is a problem that spans all sectors; solving it has to be an industry effort. If we could agree on a core set of controls and standard contract clauses, it would focus the effort in areas that most reduce risk. And free up time for suppliers and customers to work on improving security."*

Emma Smith
CISO
Vodafone



Part II: The Beginnings of Change

What will advanced third-party risk management in information security ultimately look like? It's early days but some patterns are beginning to emerge. Looking at initiatives at six companies in a range of industries, we uncovered seven types of new approaches. They are outlined in this section, starting with the ones that were most common. The case studies in Part IV provide more detail, describing how each company implemented various new approaches.

The CISOs found it was essential to gain the support of executive leadership and key stakeholders such as business units, Supply Chain Management, Procurement, and Legal. CISOs and their teams worked very closely with them in developing and implementing new approaches.

They also emphasized that driving change across a large enterprise and an ecosystem of third parties takes time. These are long-term, multi-year initiatives, not quick fixes. In all cases, the new approaches are part of a comprehensive third-party risk management program that is shifting incrementally.

THE CASE STUDIES:

"In working with third parties, a partnership model means it's not just 'we're here to assess', it's 'we're also here to help.' If you expect them to do good security, give them advice about what 'good' looks like, show them good practices. There is more willingness now on both sides to engage in this conversation."

Howard Whyte
EVP and CISO
Truist Financial Corporation

Types of New Approaches

1) Give third parties a set of top-priority security requirements.

a) Determine priority requirements.

Many companies have developed a list of priority requirements or controls. Whereas questionnaires might include hundreds of questions, the priority-based lists are often much shorter (e.g., 10 requirements). The goal is to make it easier for third parties with less mature security programs to know where to get started and to help them focus on the most effective controls.

The priorities are based on:

- Root cause analysis of past incidents, looking at both third-party incidents (where this information is available) as well as the company's own incidents, and identifying critical countermeasures.
- What controls have yielded the most risk reduction for the company's own security program.
- Security industry reports on top controls.

Some companies develop tailored prescriptive requirements for particular types of third parties. For example, a logistics provider could be required to use controls to prevent cargo theft, whereas a call center provider could be required to use controls to prevent unauthorized recordings. Other companies develop modular requirements, adding controls if the third party is handling highly

sensitive data. The list is sometimes a collaborative effort: ***Major companies in the defense industry, for example, have agreed on a list of 10 priority requirements for all suppliers.***

b) When working with third parties, center efforts around the priority requirements.

While third parties are expected to have a comprehensive set of security controls in place, companies are using their list of priority requirements–rather than questionnaires–to drive the conversation about meeting requirements and improving security. Often, the company creates regular checkpoints to hold third parties accountable. Any offers of coaching, training, and help obtaining technologies and services are designed around the priority requirements.

The case study on The Healthcare Provider shows how ***one company is replacing their questionnaire, which had 200+ self-attested controls, with 19 validated requirements***. Another case study, Tech Company B, describes an initiative which sets a deadline for the implementation of a top priority control.

2) Verify the security controls for priority requirements.

Rather than relying on third parties' self-assessments, companies are asking for evidence of security controls, especially for critical third parties. This may involve:

- Asking in-depth questions. For example, instead of asking "Do you have authentication mechanisms to manage user access?" they may ask, "Can you demonstrate that all users are using MFA to access their email?"
- Getting results of phishing tests, vulnerability scans, and penetration tests.
- Obtaining documentation such as incident response plans and software development processes.
- Asking to see an independent assessment from a qualified or certified external auditor that does an onsite audit.

Some security teams may consider scores from cybersecurity rating services for narrowly limited purposes. For instance, if the score has significantly dropped, the company will investigate the cause. Some are moving toward using automated methods of verifying controls.

In addition to verifying controls, companies are also interested in indicators of capability and maturity: Does the third party have a security leader? Is the program adequately funded? Is the program improving over time?

Reducing the Effort Spent on Questionnaires

Most companies covered in our research still ask third parties to complete cybersecurity self-assessment questionnaires and retain these records in case of future litigation and/or to meet the expectations of cyber insurers. However, many have reduced the efforts they put into review and follow up. Instead, they focus on ensuring that third parties meet the priority requirements.

3) Reduce the impact of third-party incidents.

Even third parties that are relatively good at security can have a data breach. To protect themselves from inevitable third-party incidents, companies are:

- Diversifying suppliers and increasing inventory to reduce business disruption if a supplier is inoperative due to an attack.
- Creating incident response playbooks for switching to backup suppliers in the wake of an incident.
- Developing plans to handle ransom demands.
  - Attackers sometimes target third parties with the objective of demanding a ransom from their larger customer or business partner.
- Conducting joint incident response planning and testing with key third parties.
- Ensuring the enterprise has up-to-date contact information for the security leaders of all third parties.
- Strengthening oversight mechanisms so that data sharing with third parties is limited to minimum necessary.
- Ensuring third-party access to corporate systems is minimal and can be quickly terminated.

4) Help third parties obtain security training, technology, and services.

To help their third parties improve security, companies are:

- Partnering with training service providers to offer training to third parties, in some cases helping to design the training materials and/or deliver training courses.
- Using company or industry purchasing power to offer technologies or services at a lower cost.
- Suggesting technology or service offerings that are well suited to helping their third parties meet specific security requirements (e.g., offerings tailored to a particular industry or government standard).
- Providing user-friendly instructions on how to implement priority security controls.
- Developing communications systems to rapidly deliver security alerts to all third parties.

What Forms of Assistance Can SMBs Use?

SMBs may not have the staff to make use of some types of security assistance, even if it is free.

For instance, organizations often help each other by sharing IP addresses used by threat actors, but SMBs typically lack the technical know-how to put this information to use.

CISOs in our research aimed to provide the types of help that SMBs can benefit from such as training courses on how to protect themselves from phishing attacks.

> *"Enterprises need to be continuously assessing not only their third parties' processes but also their own. Say a company sets up an agreement to share data X with the third party but then later the company ends up giving them data X plus Y. You have to hold yourself accountable for your own processes so you don't end up sharing data that you shouldn't."*

Michael Johnson
CISO
Meta Financial Technologies
Meta

5) Add incentives and enforcements to contracts.

Some initiatives to transform third-party risk management include building more incentives and/or enforcement mechanisms into contracts. How companies go about it depends on what their existing contracts look like. They may have general terms with no specific security language or language that is outdated. Updating an existing contract can take a significant amount of time and expense. New contract language tends to be adopted in phases starting with new contracts, contract renewals, and top-priority third parties.

Examples of changes to contracts that companies have made or are looking at making are:

- Setting targets for security improvements or the implementation of specific controls.
- Including rigorous security requirements that are tailored to the type of third party.
- Adding penalties for not disclosing an incident that affects the company's operations or data.
- Applying product quality incentives: Security flaws are considered product defects and suppliers must keep to an allowable defect rate.
- Offering rewards for meeting security requirements.

Contract changes require not only working closely with Legal to develop new contract language but also with the business to ensure third parties are meeting the targets outlined in the contract. An example is putting a flag on a supplier's record to say its contract should not be renewed unless security requirements are met by the renewal date.

"A possible idea for incentivizing good security is to use the concept of product quality incentives in contracts. In the purchasing agreement, you build in an allowable product defect rate. You could treat security gaps like product defects. If they have too many, they pay a penalty."

Jerry Geisler
SVP and CISO
Walmart

Some companies have chosen not to renew contracts with suppliers that failed to meet their security standards. CISOs emphasized that this is not always feasible, such as when a supplier is so deeply connected, critical, or unique that the enterprise cannot stop working with them. It also may not be feasible to uphold certain terms. For example, if an enterprise holds an SMB responsible for the costs of a breach, the costs could be more than the SMB can bear, wiping out a specialized supplier that the enterprise relies on.

6) Establish processes to increase business leaders' role in managing third-party cyber risks.

Some companies are establishing processes whereby Security provides the business with detailed information on what the cyber risks are and it's up to business leaders to:

- Heavily weigh cybersecurity risks in making purchasing decisions and forming business relationships.
- Track the risks throughout the product lifecycle or business relationship.
- Be accountable for properly weighing security risks and following up on the status of their third parties' security.

Adopting these processes requires buy-in from the business leaders, and tight integration between cybersecurity and business functions to avoid slowing the business down. Adhering to such processes is sometimes mandated by executive leadership. CISOs emphasized that this approach will also depend on organizational culture around risk acceptance, i.e., how much latitude the business has in accepting higher-risk third parties and how much they will be held accountable.

Security teams are helping business leaders recognize that each third party they add to operations adds risk to the balance sheet. The security team makes it clear how a business leader's decision to work with risky third parties could lead to potential revenue loss. For example, if a supplier with weak security is taken out by a ransomware attack and can't supply goods for days, it could reduce the business leader's quarterly closing numbers. If an insecure device is allowed on the network and is infected with malware, it could shut down one of the company's critical service offerings, resulting in loss of revenue until the system is up again.

7) Provide advanced security services to third parties.

Two of the case studies feature companies that have extended their enterprise security programs and are providing third parties with security services, including incident detection and response (The Insurance Company and The Manufacturer). This requires the company to address the liability issues of having the security team provide services to third parties. In these cases, the CISO worked extensively with Legal to develop a legal framework.

These services also involve collecting and analyzing rich data from third-party networks and systems. This requires technology to be installed on a third party's network or endpoints and methods to ensure there is no access to competitors' data.

Traditional Strategy Focused on Assessments		Broader Risk Management Strategy	
	Provide self-assessment questionnaires to third parties, asking them to declare they have a long list of controls in place.		Focus on a set of priority security requirements and verify the controls.
	Chase third parties to remediate the security gaps that were identified by the self-assessment questionnaire (often remediation doesn't happen).		Partner with third parties to help them improve their security programs.
	Focus mostly on trying to reduce the likelihood of third-party security incidents by trying to get security gaps remediated.		Assume third-party incidents will happen and place more emphasis on managing the impact of incidents on the enterprise.
	Use generic contract language holding third parties responsible for complying with regulations and standards.		Add more specific security requirements to the contract with incentives and/or enforcements for meeting the requirements.

Figure 2: Companies covered in this research are moving away from traditional strategies narrowly focused on assessments and instead devising broader risk management strategies.

"Many companies are considering ways to de-risk the business engagement with the third party from the beginning:

Be mindful of the level of connectivity between companies, thoroughly assess the controls maturity, and pursue continued visibility based on risk. Then assume there will be a security incident, test incident response plans, and discuss redundancy of providers with the business to improve resiliency.

It won't remove all risk, but you can try to de-risk as much as possible on the frontend."

Gary Harbison
CISO
Johnson & Johnson

Early Results of New Approaches

Even though these are long-term, multi-year initiatives, companies implementing new approaches are confident they are starting to reduce their third-party risk. As described in the case studies in Part IV, results are being observed in several areas:

- Avoiding third-party security incidents
  - By helping third parties be more secure and/or monitoring third-party environments, companies are avoiding third-party incidents. For example, ***one company was already able to detect and block multiple ransomware attacks*** against their third parties.
- Better use of resources
  - By shifting teams away from managing security questionnaires, companies are freeing up time to spend on more productive tasks like engaging with business teams or working with third parties on security improvements.
- Large-scale improvements in third-party security
  - Companies are finding that third parties make greater efforts to implement better security, when given achievable requirements and less arduous assessments.
  - Third parties will also readily adopt security services that are offered at the right price. Companies offering affordable services have rolled them out to hundreds or thousands of third parties.
- Lower impact on business operations
  - As companies strengthen their own resiliency against third-party incidents, they are minimizing downtime and loss of revenue. A case in point is a company that ***had over 100 significant third-party incidents over three years yet experienced only minor business disruption and costs*** due to the implementation of new approaches.

"Having a tight relationship with the business is critical for the security team in managing third-party risk. This partnership is critical not only in understanding the risk but also in responding to a potential incident that could impact the company. The business functions have the main relationship with the third party, they feel the impact the greatest. Their insight into the third party's strengths and weaknesses is key."

Kevin Tierney
VP and Chief Cybersecurity Officer
General Motors

Part III: Moving Toward Systemic Change

In discussions on transforming third-party risk management, the CISOs in the ESAF community agreed on the need for systemic change. No single company alone can solve the broader issues which range from the affordability and complexity of security controls to the lack of standardization in requirements and assessments. The CISOs identified several ways in which various organizations could help.

Technology and Security Vendors

Reflecting on why third parties are struggling with security, CISOs said time and time again that good security is too complex and expensive to implement. They called on vendors to make it possible for organizations of all sizes to achieve good security without needing highly specialized skill sets and big budgets.

Technology vendors could reduce the complexity of implementing security through measures such as:

- Have product configurations be secure by default. For instance, products should not come with default admin passwords.
- Have security features included in the base product. Vendors should not charge extra to enable features such as audit logging.
- Make it easier to use key controls such as MFA with their products.

Security vendors could offer products and services that are easier to adopt, especially for SMBs:

- Security technology should be easier to implement, particularly across heterogeneous environments and legacy systems.
- Complex security stacks are difficult to manage. Solutions should provide "security in a box" not "security in a thousand boxes."
- Offerings should be "right sized" for SMBs; they need actionable plans, clear priorities, and scalable pricing.
- Training courses need to address the needs of not only end users but also business owners who must develop security strategies.

> *"It's important that all cybersecurity professionals continue to raise the bar and innovate, not just in technology, but in processes like third-party risk management. Not doing so could potentially lead to stifling innovation in other domains."*

Catherine McCully
CISO
Procter & Gamble

Industry Collaborations

Industry collaborations can help by making good security more accessible and affordable for third parties. As discussed in the case study for The Defense Contractor, the U.S. National Defense ISAC provides members with access to resources as well as discounted pricing for cybersecurity services. Another example is the cross-industry Cyber Readiness Institute which offers free security training resources for SMBs.

Another role for industry collaborations is tackling the lack of standardization along with duplication of effort in meeting requirements and performing assessments. Companies in the same industry typically share many mutual suppliers. ISACs or informal coalitions of companies could find effective ways to harmonize requirements and assessments (see sidebar). An example is described in the case study on The Healthcare Provider: The company is working toward harmonizing and de-duplicating assessments across the healthcare industry via a service provider.

In addition to formal industry associations, large companies with mutual third parties could develop consensus statements on top-priority controls. They could also pool their resources to provide subsidized security services for smaller suppliers.

Achieving Harmonized Requirements and Assessments

Many past efforts to harmonize requirements and assessments have either not yielded agreement on the requirements or have produced extremely long lists. CISOs hope that future harmonization initiatives will provide benefits such as:

- An easier path for a third party to meet the requirements of multiple customers/partners.
- Less risk that suppliers quit and sell to less security-conscious customers instead.
- Reduced assessment effort and costs for all parties.

Governments

A key role for governments is providing education and resources to help businesses improve their security. Examples include the U.S. Cybersecurity and Infrastructure Agency's Cross-Sector Cybersecurity Performance Goals, and the UK government's Cyber Essentials.

For critical infrastructure sectors in particular, some CISOs see a role for government standards in incentivizing better security for third parties. When security regulation applies not only to the companies in these sectors but also to those companies' suppliers, it can be a forcing function for those suppliers to meet security requirements. An example in the UK is the new Telecommunications Security Act which lays out detailed security requirements covering telecom providers *and their key suppliers*. In the U.S., the Defense Federal Acquisition Regulation Supplement (DFARS) has an extensive set of cybersecurity regulations covering large defense contractors *and subcontractors*. DFARS will work in conjunction with the proposed Cybersecurity Maturity Model Certification (CMMC) to provide a mechanism for contractors *and subcontractors* to become certified as compliant with the regulations.

There is debate within the ESAF community surrounding government-led efforts to set and enforce security standards. A concern among some CISOs is that government efforts may lead to overly complex or unreasonable standards and high compliance costs. If compliance is too expensive, third parties may either leave regulated sectors or be driven out of business altogether, resulting in less innovation being available to enterprises.

Some CISOs see a role for governments in encouraging the development of secure software, such as the recent international collaboration, Shifting the Balance of Cybersecurity Risk: Principles and Approaches for Security-by-Design and -Default. This guidance provides recommendations for software manufacturers on building security into their software design processes.

Part IV: Case Studies from Six Fortune 1000 Companies

The following case studies describe initiatives at six companies where CISOs and their teams are driving new approaches in third-party risk management, working with stakeholders across their organizations and ecosystems. The initiatives are all works-in-progress and intended as food for thought for other companies looking at taking new approaches.

In all cases, the companies already had robust, mature security programs but recognized a need to evolve how they dealt with third-party cybersecurity risks. They were willing to undertake long-term, multi-year initiatives; their new approaches are part of comprehensive third-party risk management that is shifting incrementally. Each case study discusses how they got started, the practical steps they took, and key elements of their strategy.

The Defense Contractor

- Collaborating within the defense industry to prioritize controls and provide affordable security services to suppliers

The Healthcare Provider

- Streamlining security requirements and working with key vendors to improve their security practices over time

The Insurance Company

- Protecting customer data by providing security services to third-party sales associates

The Manufacturer

- Protecting the supply chain by offering security services to critical suppliers

Tech Company A

- Focusing on managing the consequences of third-party incidents

Tech Company B

- Setting a deadline for suppliers to implement a top-priority control

CASE STUDY

The Defense Contractor

Collaborating within the defense industry to prioritize controls and provide affordable security services to suppliers

Synopsis

Attacks in the U.S. defense industry are often aimed at exfiltrating intellectual property such as military equipment specifications. After observing a multi-year trend of increasing attacks on suppliers, "Defense Co" and other large defense contractors set up a task force in 2019 to make it easier for suppliers to acquire and operate military-grade security controls. Their initiative includes:

- A harmonized set of priority controls. Large defense contractors reached a consensus on 10 priority security controls for suppliers.
- Discounted or free security technologies and services made available to suppliers via the U.S. National Defense ISAC (ND-ISAC).

Suppliers are able to focus their efforts on a set of critical controls and have access to security training and a set of security service offerings, with more in progress.

Getting Started

Defense Co is a U.S. defense contractor with approximately 10,000 suppliers. More than half of its suppliers process sensitive information, and many are SMBs. The risk of confidential information theft is a critical concern not only for the company but also for national security. The defense industry has noted a multi-year trend: As the larger companies have built advanced cybersecurity programs, the attackers have increasingly targeted suppliers (see Figure 1 on page 6). To improve the security of suppliers, Defense Co is working with others in the defense industry, reflecting the closely intertwined nature of the defense industry and its long history of collaboration on cybersecurity issues.

Creation of an Industry Task Force

In 2019, Defense Co and other large defense companies (the Prime contractors), as well as U.S. government entities such as the Department of Homeland Security and National Security Agency established the CyberAssist Task Force within the Defense Industrial Base Sector Coordinating Council (DIB SCC). The goals of the task force are to help suppliers in the industry attain military-grade cyber defenses, make cybersecurity solutions available at low to no cost with a very low barrier to entry, and pool resources to support the delivery of solutions and training for suppliers.

What the Initiative Looks Like

List of Priority Controls

Defense Co and other large defense companies have developed a consensus on the top high-value controls (see below). This set of prioritized controls is used to enhance contractual and regulatory requirements. It builds additional rigor around key foundational controls and specificity on high-value Advanced Persistent Threat (APT) focused controls.

Top 10 High-Value Controls
(DIB SCC Task Force Working Group)

- Administrative Rights and Privileges
- Anti-Virus/Malware
- Default Passwords
- DNS Mitigations
- Email Filtering
- Employee Training and Awareness
- Multi-Factor Authentication
- Patching
- Perimeter Hardening
- Web Content Filtering

CASE STUDY • The Defense Contractor

Security Technologies and Services

The task force supports the U.S. National Defense ISAC (ND-ISAC) initiatives to make several security technologies and services available to defense industry suppliers at reduced or no cost. This includes an ND-ISAC Cybersecurity as a Service (CSaaS) concept demonstration funded by a Prime contractor, where commercial security vendors deliver selected services to its selected suppliers. Pilot projects underway include phishing testing and vulnerability scanning. Other technologies and services are made available through the ND-ISAC to all member companies.

Training and Documentation

The task force has developed a cohesive set of industry training packages available for defense suppliers. The large defense companies each commit to delivering training to the suppliers in a particular region. These training packages also provide training documentation such as how to configure popular applications for MFA. They are delivered by Prime contractors and others, and by the ND-ISAC through its website.

ISAC-Based Delivery Model

Multiple services are available via the ND-ISAC. Current offerings to member companies include continuous risk monitoring, email scrubber, and security awareness training. Other pilots are under ND-ISAC consideration and will depend on developing a sustainable business/funding model.

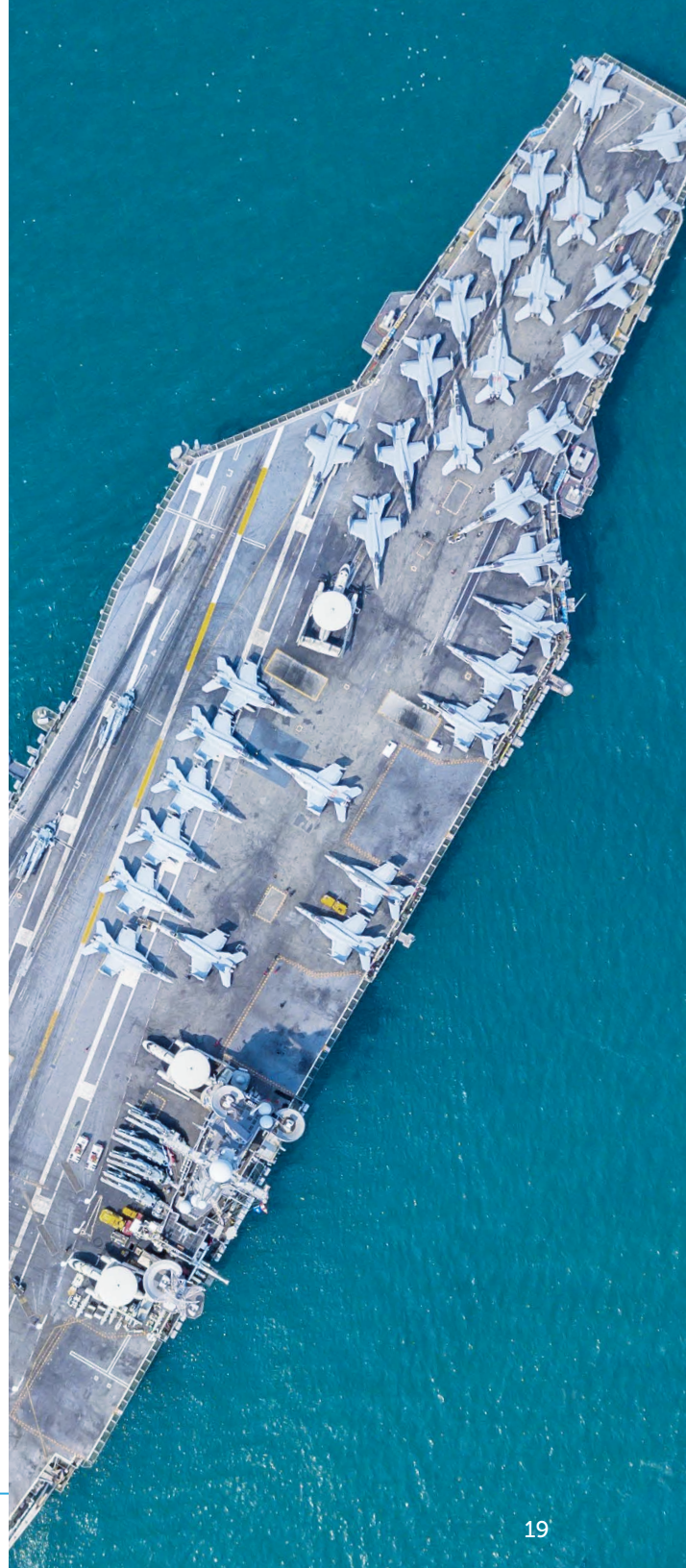
Key Elements

Industry Relationships

Relationships have been a key part of this initiative. The large companies in the defense industrial base have long had a relationship as "competimates." They have worked together for many years on cyberthreats.

Task Force Structure

Another key part has been the structure of the task force: it has a CISO oversight committee and a steering committee made up of working-level leaders from the participating companies. To participate at the voting level, a company must contribute support equivalent to two full-time employees throughout the year. Each company is responsible for providing a point person for one of the major items in the program. Agreements are all informal, soft commitments with no contracts.



CASE STUDY

The Healthcare Provider

Streamlining security requirements and working with key vendors to improve their security practices over time

Synopsis

"Health Co" operates thousands of care sites such as hospitals and medical clinics that rely on digital products to provide patient care. In 2021, an executive directive to reduce third-party risk, combined with a need to speed up procurement processes, led the CISO to begin driving an initiative to improve vendor security including:

- Requiring business leaders to help ensure that vendors they buy from meet the security standards.
- Replacing their questionnaire, which had 200+ self-attested controls, with 19 validated requirements.
- Reducing efforts spent on assessing individual products and chasing vendors regarding remediating vulnerabilities.
- Shifting efforts toward getting vendors to improve security practices in the long term.
- Outsourcing vendor risk assessments to a service provider offering amalgamated assessments for the healthcare industry.

The company has rolled out new processes for eliminating non-standard products and onboarding vendors; these processes are supported by the business at all levels. Based on current risk analysis, Health Co expects to see a 15% reduction in third-party risk exposure by the end of 2023.

Getting Started

Health Co's care sites use tens of thousands of IT and operational technology (OT) devices and systems including medical devices and patient record systems. Rapid adoption of innovative solutions is critical to patient care and competitiveness, but these solutions could be vulnerable to attacks and data theft.

In 2021, Health Co decided to re-evaluate how it was approaching vendor security to address business friction and increasing risk:

- Security assessments were slowing down procurements processes causing frustration to healthcare professionals. Assessments were very time-consuming; each product was assessed based on a 200-question questionnaire.
- After multiple potential cyber events caused by third-party incidents, the CISO reported to the executive risk committee that third-party risk was the company's number one cyber risk. The executive risk committee responded with a directive to reduce that risk.

Analysis of Issues Around Existing Third-Party Risk Management

The CISO, working with other executives, looked at how the company was currently dealing with third-party products. They found:

- Questionnaire data did not provide enough quality or depth to be able to report on third-party risk posture with confidence. For instance, questionnaires were often filled out by a vendor's sales reps rather than by technical people.
- Requirements often didn't make sense, such as "patch at a certain frequency" for legacy systems that couldn't be patched easily.
- Non-standard products not on the company's preferred list of devices had higher maintenance costs and risk.
- Often vendors would not fix security flaws that Health Co had identified.

After this analysis, they decided a radically new strategy would be needed.

CASE STUDY • The Healthcare Provider

What the Initiative Looks Like

New Gating Process for Procurement, Managed by Business Division Leaders

Business division leaders known as "capability owners" are responsible for setting the standard for products their division uses. A gating process ensures that non-standard products are not purchased without a strong business case. In gating reviews, the capability owner must be able to explain their plans for continuing to operate and recover revenue if the product incurs unexpected downtime.

The IT CFO is spearheading an effort to identify non-standard products that are currently in use. Care sites that use a non-standard product can choose to either switch to a standard product or pay the additional costs of assessing and maintaining a non-standard product.

Short List of Requirements to Replace Long Questionnaires

Health Co has shifted from assessing individual products to assessing each vendor as a company, believing that vendors with strong security practices tend to have more secure products. It has replaced a 200-question self-assessment questionnaire with 19 validated requirements (see sidebar). Health Co developed the requirements based on the root cause analyses of 20 years of security incidents and methods for assessing its own security program.

For each requirement, the vendor provides evidence to show they are meeting it. Requirements emphasize well-documented security processes, and the relevant documents are reviewed. For instance, instead of prescribing a minimum frequency for patching, the vendor is asked to describe the operations model for how it patches. Health Co would like to see indicators of maturity and trends toward better results over time.

The list of requirements is adjusted depending on the type of vendor. Once a vendor is certified, new products from the vendor can be brought in quickly. This is analogous to the U.S. TSA PreCheck program, in which participants can qualify to get expedited screening at airports. After the initial certification, vendors do an annual re-certification.

Outsourcing Vendor Risk Assessments to a Service Provider

Health Co works with a service provider that provides amalgamated assessments for the healthcare industry. With the consent of vendors, the provider shares assessment results with multiple customers, reducing duplication and saving the vendors considerable time.

Health Co's List of Vendor Security Requirements

- Application or device level penetration test
- Cloud hosting contract/security services
- Cyber liability insurance
- Dedicated security executive/leader
- Disaster recovery plan and test
- Fourth party disclosures
- Incident response plan and testing results
- Manufacturer disclosure statement for medical device security (MDS 2) (medical device only)
- Off-shore resource attestation
- Organization-level external and internal penetration tests
- PCI ROC or AOC (if in scope)
- Phishing testing
- Reportable breaches within last 18 months
- Routine secure code scanning practices
- SBOM (or list of 4th party software components)
- Secure SDLC
- Security certification (e.g., HITRUST or SOC 2 audit)
- Security implementation/ configuration documentation
- Vendor or third-party security program

CASE STUDY • The Healthcare Provider

Collaboration on Security Improvements

The CISO is working with business division leaders to make security a higher-weighted requirement in their purchasing. Health Co's 15-person vendor security assurance team has shifted its focus from managing questionnaires to:

- Working with vendors to develop better products: They use prescriptive requirements based on government healthcare standards.
- Building and maintaining an incident response portal: This contains security contact information for critical vendors so they can be quickly reached in an incident.
- Designing compensating controls: When compensating controls are needed in order for a product to be operated securely, the company works with the vendor and the assessment service provider to design controls and ensure they are implemented.
- Managing contract renewals: Contract renewal is a key lever in getting vendors to improve security. If a gap in a vendor's security practices is identified by the assessment service provider, the vendor's contract is not renewed until the problem is fixed.

By the end of 2023, based on current risk analysis, Heath Co expects to increase control effectiveness by 20% across its supplier landscape and reduce overall third-party risk exposure by 15%. Executive leadership teams from Health Co's biggest vendors have gotten on board with prioritizing security in their companies because the new approach gives them achievable requirements and relieves them from the burden of labor-intensive assessment processes. Health Co's 10,000 pre-existing suppliers are being gradually transitioned to the new assessment process, starting with the most critical 1,900 suppliers. The CISO emphasized that this is a long-term, multi-year effort.

Key Elements

Leveraging Cost-Saving Measures to Get Buy-In

Discontinuing maintenance contracts for non-standard products has helped the CISO get buy-in to the overall initiative, given the significant cost savings. The CISO realized the initial positive response could provide traction for a more comprehensive set of process changes.

Partnering with an Assessment Service Provider

The CISO plans to continue partnering with the assessment service provider, freeing up the need to use in-house resources for assessments. In the long term they envision changing the dynamics of the healthcare industry, building an industry-wide base of vendor assessment data and other security-related information. The vision is that customers will not have to pay the assessment vendor or nag suppliers to improve their security. Instead, suppliers will want to be recognized for their strong security and will pay to be assessed.

Framing Supplier Security as a Procurement Issue

The gating process for buying new products is overseen by Health Co's Ethics and Compliance team rather than by IT. The CFO gave the business division leaders a mandate to use the process, making them responsible for the risk associated with bringing products into the company.

CASE STUDY

The Insurance Company

Protecting customer data by providing security services to third-party sales associates

Synopsis

"Insurance Co" shares customer information with thousands of independent sales associates. Security gaps in their environments can put the company's data at risk.

After a series of breaches within the distribution channel, Insurance Co began an initiative in 2019 to improve the endpoint security of its sales associates and gain visibility into their security posture. In 2020, Insurance Co's own security team started providing security solutions and services:

- Endpoint scanning to ensure the endpoint meets certain security requirements (at no cost).
- An endpoint security solution with customized software and advanced security services (at low subsidized cost).

To provide a legal framework for delivering these services, Insurance Co's security organization was spun out as a separate company. Insurance Co provides endpoint security services to 2,000 associates and is gathering data on the security posture of endpoints for all 6,000 associates.

Getting Started

Insurance Co's third parties include thousands of independent agents and brokers who serve as sales associates for its products and have access to confidential customer data. Associates are typically one to three person operations with minimal security expertise. From a regulatory perspective, Insurance Co is responsible for any exposure of customer data even if the exposure is caused by an associate's breach.

Around 2018, Insurance Co's distribution channel had a series of data breaches in a short period of time. No customer data was exposed but the breaches were a wake-up call. The CISO began to investigate the possibility of leveraging their core security infrastructure to improve the security of the third parties in its distribution channel. Insurance Co has made a considerable investment in a strong centralized security model, with a central hub that responds to threat intelligence across the company.

Establishment of a Separate Entity to Overcome Legal Barriers

In discussions with executive leadership, the CISO proposed that Insurance Co's security team provide services to associates. For Insurance Co to sell security to third parties, a key factor would be to establish a legal framework which would address the liability issues. The CISO worked with the legal team and determined the best route would be to form a separate legal entity. They would spin off the security department as a separate company, with the CISO serving as CEO. The new company would carry its own insurance to cover the risk of operating as a security service provider.

Researching Feasibility and Market Demand

Insurance Co engaged an external company to conduct a feasibility study. The study found it would be feasible to structure the security department as a separate company. It also confirmed the demand for their services. Associates were spending considerable amounts of money on security products, but these products did not provide effective security. They were excited about the idea of getting security from Insurance Co's security team.

CASE STUDY • The Insurance Company

What the New Initiative Looks Like

The sales associates are small operations which typically don't have a network. Therefore, Insurance Co's security team chose to focus on endpoint security and assembled a set of technologies, services, and processes.

Endpoint Scanning

When associates log in to Insurance Co's resources, they are prompted to install software, at no cost to them, that scans their endpoints. If a machine is found to be out of compliance with security requirements, the associate can either remediate the issues themselves or sign up for the endpoint security solution (described below).

Endpoint Security Solution

Insurance Co's security team customized commercial endpoint security software and bundled this with a set of security services which they provide at a subsidized price of $15 USD per month. The solution includes next-gen AV, real-time quarantining of malware, threat intelligence, and monitoring and response.

Installation and Technical Support

The security team developed a self-service web portal and set up a call center. The web portal allows associates to download installers for security technology and to access documentation and support, making it possible to serve many non-technical users with a small number of staff.

Wide Adoption by Associates

Since the rollout in 2020, nearly all 6,000 associates have run the security scan and 2,000 are using the optional endpoint security solution. The program has blocked multiple ransomware attacks, improved performance through the detection and removal of unwanted software, and provided high user satisfaction.

Key Elements

Pilot Project and Phased Delivery

A pilot project with 50 associates was key for the initiative. Insurance Co's security team was able to develop processes to solve issues discovered during the pilot, such as installation issues, before scaling up the program.

Startup Model for Staffing

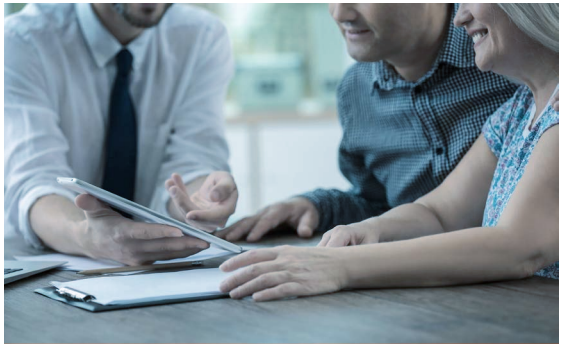
The CISO approached the initiative along the lines of running a small startup company and therefore hired people with startup skills. The individual hired to lead the initiative had a background in professional security services, including creating, pricing, marketing, and selling products. The person also had years of technology experience in engineering, support, and sales engineering. The CISO reports that the initiative has been a "fun" and "fantastic" experience for Insurance Co's security team.

Reducing Risk, Not Making a Profit

Insurance Co's leadership agreed from the start that the purpose of providing security to third parties was risk reduction, not profit.

Subsequently, they have discussed increasing prices for their security services in order to make a profit but have chosen to continue to operate it on a break-even or subsidized basis. The service delivers enough value to the company by increasing security for current associates and attracting new ones.

In the long term, the CISO envisions an industry effort whereby the Financial Services ISAC might take over the program. Having analyzed what associates are willing to pay and what the services cost to deliver, the CISO thinks a non-profit organization such as an ISAC would be the most suitable home for it.



CASE STUDY

The Manufacturer

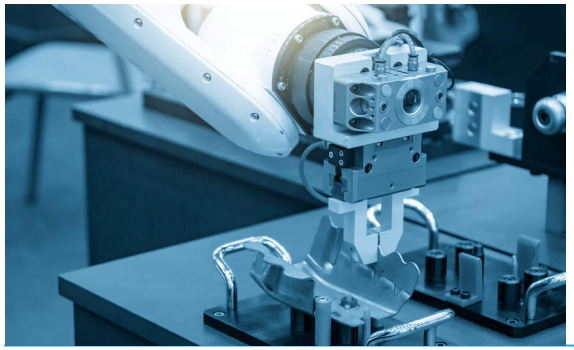
Protecting the supply chain by offering security services to critical suppliers

Synopsis

In 2018, "Manu Co" began an initiative to improve the security posture of high priority suppliers. Urgency increased after a series of ransomware attacks led to business disruption and auditor questions. In 2019, unable to find a suitable commercial solution, Manu Co's security team began to offer services to key suppliers including:

- Advanced cyber defense services such as 24/7 incident detection and response.
- Threat hunting operations. Monitoring suppliers' environments enables Manu Co's security team to gather rich data for threat intelligence.
- Recommendations and training.

Services are delivered through a value-added reseller (VAR), which provides the legal framework for operating as a service provider. Manu Co is providing advanced security services to around 150 suppliers and aims to serve 2,000.



Getting Started

Manu Co incorporates components from 9,000 suppliers into its products, for which safety and reliability are critical. Its top third-party cyber risks include faulty or compromised components, production line stoppage, and intellectual property (IP) theft.

In 2019, the company's suppliers were hit by a series of ransomware attacks. Manu Co's existing third-party risk management strategy included a comprehensive product architecture and testing program so no single supplier failure can result in insecure products. However, the escalation of attacks on suppliers led Manu Co to investigate ways it could help suppliers improve their cyber defenses. In discussions with suppliers, Manu Co found they were struggling to find qualified security talent to hire and to fund and sustain cybersecurity programs.

Commercial Services Not Suitable

Initially, Manu Co's security team looked into finding a managed security services provider (MSSP) that its suppliers could use to improve their cyber defenses. It inquired with the suppliers that were already using MSSPs and discovered that the suppliers were not achieving effective security. Issues included overly high prices and no clear definition of services. Cost-conscious suppliers often negotiated on price to the extent that the scope of services was reduced to an inadequate level.

Manu Co's security team concluded that MSSPs weren't able to provide the quality or scale the suppliers needed at a cost they could afford. Therefore, the company decided to develop a program which would extend its internal security services to suppliers. The idea of having Manu Co provide services to suppliers initially came from suppliers themselves; they recognized Manu Co's security expertise and wanted to benefit from Manu Co's capabilities.

Motivated by the Sheer Volume of Attacks

In the two years before Manu Co began to help suppliers with security, Manu Co's suppliers incurred 50 significant incidents, nearly all of which were ransomware. Some of these disrupted Manu Co's business when suppliers were temporarily unable to provide parts or services. Others involved targeted IP theft. In each of these 50 incidents, besides the business disruptions, Manu Co had to answer multi-page questionnaires from auditors.

Although initially reluctant to extend security services to its suppliers, Manu Co found that the sheer volume of attacks and auditor questions led it to reconsider. Navigating the legal and financial issues around extending their services would turn out to be lower friction than dealing with the rate of supplier incidents.

CASE STUDY • The Manufacturer

Using a Value-Added Reseller (VAR) to Overcome Legal Barriers

Before providing services to suppliers, the CISO spent months negotiating with Legal to determine a legal framework to deal with the liability issues. Manu Co had to ensure that the company would not be held responsible for any supplier problems such as product security flaws or failure to deliver products.

Manu Co established a model whereby it would offer security services through the company's existing VAR. The company had close ties to the VAR and partial ownership. For this initiative, the VAR operates as the official service provider while Manu Co's staff do the actual security work. This ensures a level of legal and financial separation. Services are provided at cost by Manu Co, with a nominal profit margin for the VAR. The VAR owns the services contract with the suppliers and carries insurance to cover the risk.

What the New Initiative Looks Like

Advanced Cyber Defense Services and Threat Hunting

Manu Co's security services program provides Security Operations Center (SOC) capabilities consisting of 24/7 threat intelligence, incident detection, and event monitoring; attack surface management (a combination of threat and vulnerability management); and incident response.

By gathering data from suppliers' environments, Manu Co's security team gains deep visibility into their suppliers' security posture. These insights enable Manu Co and its suppliers to better outmaneuver threats. Manu Co's security team also helps suppliers improve their security controls by providing guidance and training on controls implementation.

Aiming for 2,000 Suppliers

Since rolling out the service, about 150 suppliers have been onboarded and Manu Co's security team is aiming for 2,000. Satisfaction with the program is high for both Manu Co and suppliers. Manu Co's CISO notes that the arrangement gives suppliers a world-class security team at scale and at cost. The goal will continue to be improving security and reducing supply chain risk, not profiting from selling security.

Key Elements

Pre-Existing Scaled Services Team

A prerequisite for the initiative was that Manu Co's security team was already able to run internal services at scale. The team consists of 150 people serving the majority of their worldwide footprint. Two leaders with professional services and sales experience were added to the security team.

Protecting Confidentiality of Competitors' Data

One of the biggest challenges has been working with suppliers that also supply Manu Co's competitors and handle proprietary information from those competitors. In most of these cases the solution was data segregation; Manu Co's security team is able to scan for vulnerabilities and check logs but is not able to look at the data. Where data segregation was not feasible, Manu Co had discussions with the legal and security teams of its competitors and, in most cases, was able to find another solution.

Prioritizing Suppliers for Services

Manu Co's security team prioritizes suppliers that are the most critical from a business perspective. If a supplier is critical but declines to participate, Manu Co flags the supplier for more attention in assessment processes.

Suppliers are also prioritized by their level of readiness. To be served by the program, the supplier's IT environment must support logging and other modern security functions. Manu Co brought in service providers to help some suppliers implement the required newer technology.

CASE STUDY

Tech Company A

Focusing on managing the consequences of the third-party incidents

Synopsis

"Tech Co A" relies heavily on its supply chain. In 2020, it undertook a complete reassessment of its third-party risk management strategy, shifting spending away from questionnaire-based assessments and toward more effective methods which include:

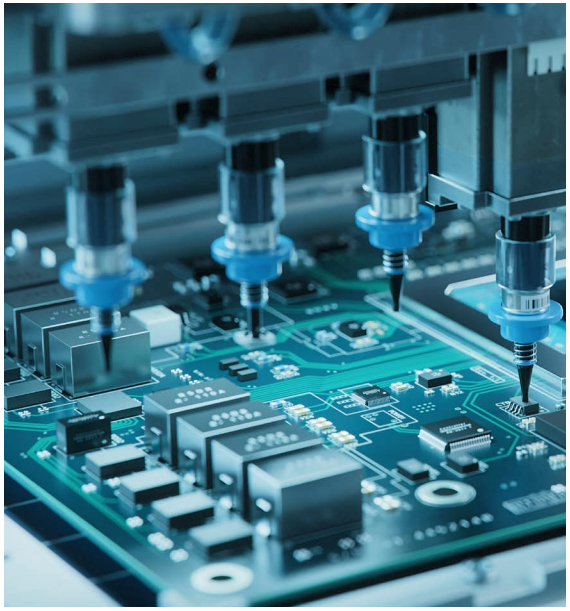
- Building a comprehensive strategy based on key risk scenarios, focusing as much on business controls (contracts, supplier diversification, etc.) as on traditional security controls.
- Extreme security requirements and controls assurance for top-tier suppliers such as hardware and software developers whose components are incorporated into products.
- Emphasis on business continuity planning for the vast majority of suppliers, with an aim to reduce the impact of incidents rather than the likelihood.
- Integrating security into business governance processes, with risks owned by business leaders.

To gauge the success of third-party risk management, the CISO looks at the business impact of third-party incidents rather than incident rates. Despite having experienced over 100 significant third-party incidents in three years, none have resulted in more than minor business disruption or cost.

Getting Started

Supply chain resiliency is a corporate priority at Tech Co A. The company relies on tens of thousands of suppliers around the world, which provide hardware and software components, logistics, and services at scale. The top third-party cyber risks that the company faces are business disruption due to supplier downtime, loss of IP held by the supplier, and product compromise.

Between 2019 and 2022, the company saw a 550% increase in third-party incidents. In the early stages of this trend, Tech Co A began a complete re-evaluation of its third-party risk management strategy to maximize risk reduction.



Analysis of Traditional Methods Uncovers Significant Issues

Tech Co A's research found that its traditional methods were highly wasteful and led to a false sense of precision and confidence. Findings included:

- Questionnaires slow down procurement processes and use a lot of security team time.
- Security bureaucracy increases costs for third parties, which are reflected in higher prices.
- Questionnaire data is based on self-attestation and is therefore unreliable.
- Most third-party cybersecurity rating services gather data from limited internet-footprint snapshots and are not able to indicate how secure a third party actually is.
- In the absence of meaningful data on third-party security posture, reports to senior leadership tend to be based on poor-quality data.
- Most financial costs incurred from third-party incidents were due to business operational outages rather than data loss.
- When companies incur losses due to a third-party incident, they seldom recover costs from the third party.

CASE STUDY • Tech Company A

What the Initiative Looks Like

Comprehensive Strategy for Key Risk Scenarios

Tech Co A developed a new third-party risk strategy that has been implemented over several years and involves changing multiple business processes. The CISO emphasizes the need to use diverse methods to reduce third-party risk.

Three major risk scenarios, shown in the following table, illustrate key elements of the strategy.

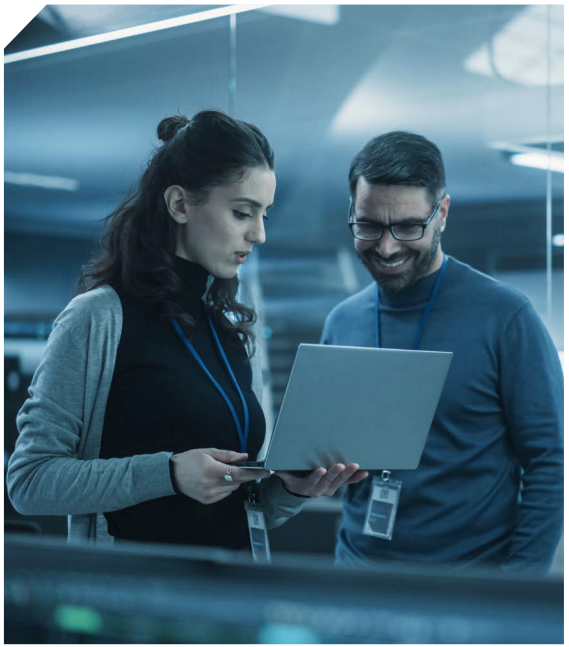
Risk scenario	Primary controls	Secondary controls	Tertiary controls
Downtime due to cyber or physical world event	Supplier diversification and associated business continuity planning	Contractual liability transfer to third party	n/a
Third-party loss of Tech Co A sensitive data	Limiting information shared	Contractual liability transfer to third party	Data deletion requirements *(All third parties are contractually required to delete all information supplied by Tech Co A after 30 days. Exceptions require approval from a senior executive and are formally inventoried.)*
Third party hacked, leading to supply chain attack on Tech Co A customers	Technical controls at Tech Co A to vet third-party code	Limiting use of third-party code	Extreme security requirements levied and enforced

Extreme Security Requirements for Highest-Priority Suppliers

Tech Co A's highest-priority suppliers develop sensitive hardware and software that are built into Tech Co A's products, and/or work with highly confidential data. For these suppliers, Tech Co A takes what the CISO describes as "excruciating" efforts to ensure suppliers are not compromised including:

- Prescriptive requirements tailored to the supplier in custom contract language.
- Audits and site visits to validate that requirements are met, with specific questions to evaluate controls in depth.
- Annual summit at company headquarters where top-tier suppliers meet with senior Tech Co A leadership.

Tech Co A has chosen not to renew contracts with some major suppliers—including billion-dollar companies—that failed to meet the standards it has set to ensure product integrity.



Tailoring Requirements to the Supplier

In contracts with top-tier suppliers, Tech Co A prescribes specific requirements to mitigate the relevant risks. For example:

- To safeguard customer privacy, a call center must not allow employees to bring personal recording devices to their desks.
- To prevent cargo theft, a logistics company must not allow its drivers to stop in certain high-theft areas.

CASE STUDY • Tech Company A

Emphasis on Business Continuity Planning

Tech Co A realized that, for most third parties, it is futile to try to decrease the likelihood of incidents. In an inversion of previous priorities, the company has reduced the attention paid to assessments for most suppliers. It now assumes incidents will happen and prepares to manage the consequences.

For most suppliers, the primary type of risk is availability risk—an incident at a supplier could potentially cause interruption in delivery of goods or services. The company found that business continuity planning (BCP) yields a high return on investment in mitigating this risk. It increased BCP spending tenfold with efforts that include:

- Supplier diversification to ensure that no supplier is a single point of failure.
  - For instance, if customer service in a particular country is outsourced, it is outsourced to multiple providers and each one must agree to ramp up capacity if another provider goes down.
- Digitizing all business continuity plans and integrating the business continuity planning system with the third-party procurement system.
- Playbooks to bring on backup suppliers in the wake of an incident.

Business Governance Processes

Each third party has a sponsoring business leader at Tech Co A who makes build-vs-buy decisions:

- The business leader owns the risks associated with using a third party.
- The security team works with business leaders to help them understand that every third party adds risk to the balance sheet.
- Business leaders use scorecards in managing the overall relationship with suppliers. For example, the scorecards are used in CEO-level meetings and quarterly reviews. The scorecards include not only business goals but also information on the third party's security posture.

Measuring Success by Business Impact

To gauge the success of third-party risk management, the CISO looks at the business impact of third-party incidents rather than incident rates. ***In the three years since Tech Co A overhauled its approach, it has experienced over 100 significant third-party incidents, none of which resulted in more than minor business disruption or cost.***

Key Elements

Organizational Structure and Culture

The third-party risk management initiative is enabled by Tech Co A's organizational structure and culture. The company has a decades-long commitment to supply chain resiliency. Business continuity has recently been globalized and integrated with security into a single resiliency/security program. And business leaders own the risk associated with third parties that they choose to engage.

Third-Party Resiliency Team

Tech Co A's CISO built a multi-disciplinary third-party resiliency team. It produces valuable data that is used to steer funding decisions. Team member backgrounds include technology, business continuity, and cyberthreat analysis. The team developed a digitized and interconnected process that rates the criticality of third parties and other key assets and maps their dependencies. This process enables single-point risk identification.

In-depth Inquiries

Traditional security questionnaires have questions such as "Do you use a secure product lifecycle process?" and "Do you do phishing testing?"

Tech Co A's CISO explains that these questions are not deep enough to indicate whether an organization's controls are effective. It's too easy to say yes to everything.

With top-priority suppliers, Tech Co asks more specific questions such as, "How often do you do vulnerability scanning and what are the results?"

CASE STUDY

Tech Company B

Setting a deadline for suppliers to implement a top-priority control

Synopsis

After ransomware attacks on suppliers, "Tech Co B" began a major initiative in 2021 to improve supplier security, with a focus on SMB suppliers. The initiative includes:

- Top-priority focus areas for supplier security: A list of six areas described in simple language.
- Deadline for meeting a top priority security requirement: All suppliers must implement MFA by 2025.
- Security training: Suppliers can access resources designed in conjunction with a training institute.
- Incident preparedness: Enhanced processes to protect Tech Co B in the event of a third-party incident.

The security team has gained buy-in across the entire company for improving supplier security, including the deadline for suppliers to implement MFA. They are working in collaboration with the procurement team and other corporate stakeholders to ensure suppliers can meet the deadline.

Getting Started

Tech Co B's 25,000 suppliers range from manufacturers to providers of services such as facilities maintenance and marketing. Many critical suppliers are SMBs. Attacks on suppliers could result in loss of IP or personal data, network compromise, or business disruption.

In 2021, suppliers were hit with ransomware attacks in which the attackers were aiming for Tech Co B's data. This drove home the fact that attackers are deliberately attacking small suppliers in order to get to their larger customers. Large enterprises like Tech Co B have made significant investments in security and implemented more advanced strategies, so they have become more difficult targets. With less sophisticated security capabilities, SMB suppliers are easier and faster to compromise. This motivated Tech Co B to begin an initiative to help SMB suppliers improve their security.

Looking into the State of Supplier Security

Tech Co B started by doing some research on their suppliers' security. To collect candid information from their suppliers, the company conducted an anonymous survey asking 5,000 suppliers simple questions about their security controls. The research also included a root cause analysis of the recent ransomware attacks and a review of supplier security assessments.

Common issues were lack of MFA, inadequate use of vulnerability scanning, no formal security team or response process, unpatched or end-of-life systems, and no centralized logging. Another finding was that many SMB suppliers are non-technical and find security requirements as outlined in regulations and standards (such as HIPAA, SOX, and PCI) too long, complex, and full of jargon and convoluted language.

CASE STUDY • Tech Company B

What the Initiative Looks Like

Top-Priority Focus Areas for Supplier Security

The company decided to provide a simplified, boiled-down explanation of security requirements to their suppliers. This consists of six top-priority focus areas (see sidebar), described in plain language that non-technical people can understand. Suppliers are contractually obligated to comply with regulations and standards, however, for purposes of assessment and training, the company focuses on the six areas.

MFA is the number one priority. This was decided for several reasons including:

- A Microsoft report estimated 99.9% of account compromise attacks would be prevented with MFA.
- MFA technologies are widely available and in many cases are relatively simple to enable.
- Many enterprises consider MFA a key control and have implemented it for access to corporate resources.
- If other large enterprises and influential customers joined in communicating this to suppliers, they might move faster to implement it.

The company's research had found several factors hindering MFA usage including lack of awareness, cost, and perceived complexity. In many cases suppliers already had the technology to use MFA but had not turned it on.

Tech Co B's Top-Priority Focus Areas for Supplier Security

- MFA (#1 priority)
- Event logging
- Incident response
- Resiliency
- Security training
- Vulnerability management

Deadline for Suppliers to Implement MFA

Tech Co B's CISO decided that having a deadline was key to persuading suppliers to implement MFA. In 2022, the company announced that all suppliers must use MFA by 2025. For suppliers that do not meet this requirement by 2025, Tech Co B will strongly consider severing ties with that supplier. In conjunction with the deadline, the company's strategy also involves:

- Devoting resources such as training, coaching, and targeted subsidies to help suppliers meet the deadline.
- Communicating repeatedly with suppliers.
- Exploring ways to technically verify whether a supplier has specific security controls in place.

Security Training for Suppliers

Tech Co B developed a Supplier Security Guidance document explaining the six focus areas in plain language. It also partnered with a non-profit training organization, the Cyber Readiness Institute (CRI), to provide training materials covering the focus areas. Tech Co B promotes CRI training to its suppliers and recognizes CRI certification in its assessment processes. For instance, to show that it meets Tech Co B's requirements for incident response (IR) planning, a supplier can provide evidence of CRI certification in IR and a copy of its IR plan.

MFA by 2025

Suppliers must use MFA on:

- Collaboration tools
- Email
- Payment systems
- Privileged accounts
- Remote corporate access/VPN
- Social media accounts

MFA is defined as "anything more than a password." Any tool or method of MFA qualifies, including device registration or SMS. This is intended to give a manageable initial scope for 2025, with the possibility of increased stringency in the future.

CASE STUDY • Tech Company B

Assistance in Meeting Requirements

Tech Co B is investigating models for making security technologies and services more widely affordable and feasible. For instance, a pilot project in 2023 is following the journeys of eight suppliers as they implement MFA. Tech Co B will collect data on what it takes for an SMB to implement MFA, see what support SMBs need, and evaluate MFA vendors.

Increased Incident Response Preparedness

Tech Co B has developed more detailed plans for responding to cyber attacks on third parties, including handling ransom demands. It has put together a database of supplier information to ensure that staff can quickly find the supplier's security contact person, the contract, and the latest assessment results in case of a security issue. Tech Co B has also put a rapid communication system in place to ensure that, in the event of an incident with one supplier, the company can promptly alert all other suppliers and advise them.

Messaging and Contracts

The security team found that the most effective way to get their educational messages to thousands of suppliers was to have front-line procurement and finance staff deliver them. Typically emails from these groups are read whereas emails from the security team are often ignored. Messages about strengthening security defenses are repeated in the company's public messaging and in every type of interaction the company has with its suppliers.

Tech Co B added language to its Supplier Code of Conduct to include consequences for non-compliance with security requirements. It is updating security language in contracts with new suppliers, and with existing suppliers when contracts are up for renewal.

Specific Controls vs Checklist Approaches

Tech Co B's new approach to assessing supplier security exemplifies a shift that several CISOs in our research are making. Instead of relying on traditional assessment methods such as SOC 2 audits reports, CISOs are getting much more specific about what controls they want to see.

Since SOC 2 audit reports reflect compliance rather than security, a company can pass a SOC 2 audit while still lacking fundamentals such as the use of MFA for email. Tech Co B uses MFA as a filter to see if it is worth assessing a supplier's security any further. The CISO puts it this way: *"If you don't have MFA, I don't even want to look at your SOC 2 report."*

Key Elements

Wide-Reaching Internal Persuasion Campaign

A key part of this initiative has been an internal communications campaign to get stakeholders to embrace the vision for improving suppliers' security posture, including the deadline for meeting MFA requirements. The security team worked with stakeholders across the organization, including Legal, Procurement, and PR, and gained the backing of the company up to its highest levels including the CEO and board. The security team also engaged directly with front-line staff in Procurement and Finance rather than expecting messages to trickle down from executives.

Initially there was pushback from some stakeholders, especially regarding the deadline for suppliers to implement MFA. To handle objections, the security team emphasized that most suppliers want to be more secure and that efforts are being made to make security easier for suppliers.

Partnering with SMB Suppliers

In helping SMB suppliers to improve their security, Tech Co B is investing a lot of effort into understanding the suppliers' point of view. The company is engaging deeply with their suppliers to fully grasp their challenges. In designing new approaches, Tech Co B considers how to share their own security team's knowledge and skills with suppliers and find ways to lessen financial and practical barriers to security.

Biographies: RSAC ESAF 2023 Program Committee

Zaki Abbas

Senior Vice President,
Chief Information Security Officer

Brookfield Asset Management

Zaki is currently CISO at Brookfield Asset Management, a leading global asset management company based in Toronto, Canada, with over $800 billion of assets under management. He has over 15 years of experience in information security. Prior to joining Brookfield, Zaki was Assistant Vice President of Information Security at Economical Insurance and worked as an Information Security Officer at Great-West Life and an Information Security Advocate at IBM. Zaki holds a bachelor's degree in computer science and economics from York University.

Brad Arkin

Senior Vice President,
Chief Security and Trust Officer

Cisco

Brad leads Cisco's Security and Trust Organization, whose core mission is to ensure Cisco meets its security and privacy obligations to customers, regulators, employees, and other stakeholders. Previously he was Chief Security Officer at Adobe and has held management positions at @Stake and Cigital. He holds a B.S. in computer science and mathematics from the College of William and Mary, MS in computer science from GWU, and MBA from Columbia University and London Business School.

Jason Barnett

Vice President,
Chief Security Officer

HCA Healthcare

Jason has spent more than 25 years in the technology field, with a primary focus on threat detection and response. Now, as the Chief Security Officer for HCA Healthcare, he leads a converged program that includes Cyber Security, Physical Security, Privacy, Identity Engagement, and Business Risk Solutions that protect the company's 186 hospitals, more than 2,000 outpatient and physician clinics, 260,000 employees, and 31 million patient encounters each year.

BIOGRAPHIES • RSAC ESAF 2023 Program Committee

Benjamin Brophy

Group Chief Information Technology and Security Officer

Reckitt Benckiser Group

Ben leads global technology and security at Reckitt, a British multi-national consumer goods company. He has over 20 years of experience in technology and information security across multiple industries. Previously, Ben was CISO at Bankwest and held senior security consulting roles at PwC, Accenture, Friends Life Group, and Synergy. Earlier in his career, Ben had operational security roles at Network Rail and the UCL Institute of Education. He has a Master of Science degree from Royal Holloway, University of London.

Deneen DeFiore

Vice President and Chief Information Security Officer

United Airlines

Deneen is responsible for leading United's cybersecurity and digital risk organization. She leads initiatives on commercial aviation cyber safety risk, improving cyber resilience, and reducing cyber safety risk world-wide across the aviation ecosystem. Deneen is board chair of Aviation Information Sharing Analysis Center and chairperson of Airlines for America (A4A) Cybersecurity Committee. In 2022, she was appointed to the President's National Infrastructure Advisory Council (NIAC), advising the White House on improving security and resilience of the nation's critical infrastructure sectors.

Jerry R. Geisler III

Senior Vice President and Chief Information Security Officer

Walmart

Jerry leads Walmart's global information security department. His responsibilities encompass data security not only for Walmart's 230 million customers but also its 2.3 million associates. He oversees information security strategy, engineering, operations, services, testing and assessment, risk, governance, and compliance for the global enterprise. Under Jerry's leadership, Walmart's information security program is considered a forward-thinking industry leader focused on emerging best-in-class information security practices, innovation, and business enablement broadly engaged across IT, ICS, cloud, platform, and product security domains.

BIOGRAPHIES • RSAC ESAF 2023 Program Committee

Richard A. Hale

Global Chief Information Security Officer

Sony Group Corporation

Richard currently leads Sony's global information security effort. Previously he had various cybersecurity jobs in the U.S. Government, finishing as the Department of Defense CISO. While in the government, Richard helped develop some of the foundational cybersecurity approaches within government that have become global industry best practices.

Gary Harbison

Chief Information Security Officer

Johnson & Johnson

Gary is the Chief Information Security Officer at Johnson & Johnson with global ownership of managing enterprise technological risks, protecting company data and information and leading cybersecurity transformation at one of the world's largest healthcare companies. Previously, Gary was Global CISO at Bayer. He has 28 years of overall IT experience, mostly focused within the cybersecurity domain, including with multiple global Fortune 500 companies, as well as public sector experience with the U.S. Department of Defense.

Katie Jenkins

Executive Vice President for Global Cybersecurity and Chief Information Security Officer

Liberty Mutual Insurance

Katie is responsible for the global cybersecurity program, ensuring protection of company data, defense of the brand and minimizing business impact of cyberattacks. She leads enterprise cybersecurity policy, strategy and programs. Prior to this role, Katie was Vice President and Senior Director, leading cloud and security enablement programs for Liberty's commercial insurance division. Her previous information security experience includes positions with AT&T Consulting Solutions, VeriSign, Guardent and PWC.

BIOGRAPHIES • RSAC ESAF 2023 Program Committee

Michael Johnson

Chief Information Security Officer

Meta Financial Technologies, Meta

Michael oversees security for Meta's payments and financial services, and leads Governance, Risk, and Compliance supporting security, integrity, and support. Previously, Michael was SVP / CISO at Capital One, Chief Information Officer for the U.S. Department of Energy, and served in other key cyber-focused executive roles in the U.S. Government at the Office of the Director of National Intelligence, U.S. Department of Homeland Security, and White House Executive Office of the President.

Catherine McCully

Chief Information Security Officer

Procter & Gamble

Catherine oversees cybersecurity and information security for P&G's global enterprise. She leads the organization responsible for establishing and maintaining strong protection for P&G, while enabling business operations and growth with a focus on secure, resilient capabilities. Prior to P&G, Catherine held several cybersecurity and information security roles in global financial services and retail Fortune 100 companies. Her experience ranges from engineering to risk management, and frontline incident response to key leadership roles overseeing transformative changes.

Michael McNeil

Senior Vice President,
Global Chief Information Security Officer

McKesson

Michael is responsible for enhancing and overseeing McKesson's information and operational technology security strategy program and managing information security governance. Previously he was Global Product Security and Services Officer for Royal Philips and held senior leadership positions at Medtronic, Liberty Mutual Group, Pitney Bowes, and Reynolds & Reynolds. He holds several board and executive member positions, including the Healthcare and Public Health Sector Coordinating Council (HSCC) Executive Committee and the Health Information Sharing and Analysis Center (H-ISAC).

BIOGRAPHIES • RSAC ESAF 2023 Program Committee

John Scimone

President and Chief Security Officer

Dell Technologies

As Dell Technologies' Chief Security Officer, John is responsible for the company's global security, privacy and resiliency programs spanning the physical and cyber domains. Previously, John was Global CISO at Sony Group, and has held leadership roles with the U.S. Department of Defense, including Director of Security Operations for the Secretary of Defense's communications office. John holds a bachelor's degree in computer science and a master's in strategic intelligence studies.

Emma Smith

Chief Information Security Officer

Vodafone

Emma leads cybersecurity globally at Vodafone, alongside Technology Strategy and Assurance. The cybersecurity team sets risk appetite and policy, manages security risk, defines security architecture, assures product and service security, delivers and operates security tools, and runs global 24/7 cyber defence capabilities. Emma is passionate about security and an active sponsor for diversity and inclusion in the workplace. She also holds an independent Security Advisor role for a UK retail company and sits on the UK Cabinet Office National Cyber Advisory Board.

Kevin Tierney

Vice President and
Chief Cybersecurity Officer

General Motors

Kevin is responsible for all aspects of cybersecurity throughout General Motors. He leads enterprise, product, and manufacturing cybersecurity programs, with a focus on security architecture, penetration testing, cyber risk management, incident response, vulnerability management, intelligence, awareness and training, and governance. Prior to his current role at GM, Kevin served as the Chief Product Cybersecurity Officer and Director, Vehicle Architecture Cybersecurity. Kevin also currently serves as Vice-Chair of the Automotive Information Sharing & Analysis Center (Auto-ISAC).

BIOGRAPHIES • RSAC ESAF 2023 Program Committee

Howard Whyte

Executive Vice President and
Chief Information Security Officer

Truist Financial Corporation

Howard is responsible for executing the corporation's information security program and aligning with enterprise programs and business objectives, ensuring information assets and technologies are protected. Previously, he was CISO at Boeing. He has worked for 20+ years as an executive leader of information technology and security including as Chief Information Officer and Chief Privacy Officer and CISO at the Federal Deposit Insurance Corporation (FDIC), leader of Goldman Sachs' Threat Management Center, CISO at NASA, and senior information officer in the U.S. Army.

JR Williamson

Senior Vice President and
Chief Information Security Officer

Leidos

JR is accountable for information security strategy, business enablement, governance, risk, cybersecurity operations, and classified IT at Leidos. He is a CISSP, Six Sigma Black Belt, and serves on the Microsoft CSO Council, the Security 50, Gartner Advisory Board, the Executive Security Action Forum Program Committee, DIB Sector Coordinating Council, WashingtonExec CISOs, Evanta CISO Council, the National Security Agency Enduring Security Framework team, and is the Chairman of the Board of the Internet Security Alliance.

To sign up for emails from RSA Conference that include reports like this, please go to:

www.rsaconference.com/signup